UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

UNITED STATES OF AMERICA	)	
	)	
v.	)	CASE NO.: 8:24-CR-211-TDC
	)	
HOAU-YAN WANG,	)	
	)	
Defendant.	)	

DEFENDANT HOAU-YAN WANG'S BRIEF IN SUPPORT OF MOTION IN LIMINE TO EXCLUDE TESTIMONY OR REFERENCES TO IMAGES AS SOURCE IMAGES

Defendant Hoau-Yan Wang ("Dr. Wang") respectfully moves this Court to prohibit the Government from eliciting testimony, admitting exhibits, referring to in opening statements or closing arguments, or in any other way alluding or referring to images obtained from Dr. Wang as "source or original images" of certain images submitted in grant applications to the National Institute of Health ("NIH") unless and until this Court determines outside the presence of the jury that the Government has met its burden to authenticate such images as source images under Federal Rule of Evidence ("FRE") 901. In support, Dr. Wang respectfully provides the following:

BACKGROUND

From 2005 to 2023, during his employment at the City University of New York ("CUNY"), Dr. Wang conducted Alzheimer's drug research for Cassava Sciences, Inc. ("Cassava") using several laboratory techniques, including a protein detection technique called Western blotting, on animal and human postmortem brain tissues and human body fluids. (Doc. 1 ¶ 9). Western blotting is a largely visual laboratory technique that allows a trained scientist to detect a specific protein by developing and analyzing a visible "band" on physical x-ray film. (*Id.*). That film is then digitized using a scanner and can be enhanced for publication and submission as part of grant applications. (*Id.*). (The permissible scope of that enhancement is the real issue in this case). Separate from the

visual image of a Western blot "band," the test's results can be quantified using a process called densitometry, which compares the darkness and thickness of various bands to determine the relative protein amounts in each sample. (*Id*.).

Cassava applied for grants from the National Institute of Health ("NIH") to fund its research. (*See id*. ¶ 10). Grant applications require detailed, comprehensive information about Cassava's research projects. (*Id.* ¶ 6). Cassava included representative Western blot images in its applications. (*See, e.g., id*. ¶ 18 (providing an example of an allegedly manipulated Western blot)). The Government's indictment accuses Dr. Wang of manipulating Western blot images submitted by Cassava in NIH applications. (*See, e.g., id*. ¶ 14.c). The Government's case turns on whether it can link specific, allegedly manipulated images submitted in NIH applications to other images gleaned from Dr. Wang's devices. That burden is substantial—and unlikely to be met.

First, the Government cannot establish any digital continuity between the supposed source files and the NIH-submitted images. The supposed "source images" and the NIH-submitted images do not share the forensic markers needed to prove such a connection. As discussed in the expert report of Alyssa Lisiewski, the Western blot films were initially scanned into .tiff format, then converted through ImageJ to JPEG files to facilitate densitometry analysis, cropped and adjusted in Photoshop, and ultimately assembled into labeled panels in PowerPoint for transmission. (Ex. 1 at 3-4). By the time the figures were embedded and saved in PowerPoint, the component images had been flattened into a composite with no independent identifiers, no recoverable metadata, and no hash values or digital fingerprints, making it impossible for the Government to forensically trace back from the NIH image to a source image. (*Id.* at 6-10). In short, the Government cannot demonstrate in a forensically sound manner that any of the images it now seeks to rely upon are the actual "source files" of the NIH submissions.

Second, the Government has not proffered any witness with personal knowledge who can attest that the extracted images are in fact the same images forwarded to the NIH. According to FBI 302s disclosed by the Government in discovery, two post-doctoral researchers who were part of Dr. Wang's lab during portions of the period covered by the indictment have unequivocally stated that they had no involvement in the digitization or formatting of the images, and only limited, if any, involvement in the underlying Western blot preparation prior to digitization. And, the Government offers no other witnesses to fill that evidentiary gap. Nor does the Government offer evidence obtained via search warrant from CUNY because it chose not to conduct such a search, but merely relied on CUNY to produce subpoena returns that were not fulsome enough to include the necessary evidence.

Further destroying the chain of custody, Dr. Wang did not submit the grant applications at issue; they were submitted by Cassava—a third party located half-way across the country from Dr. Wang's lab. (Doc. 1 ¶ 10). Cassava inserted all of the Western blot images into the applications it submitted to the NIH. (*Id.*). Cassava's key personnel—based in Austin, Texas—were geographically and operationally removed from the creation and digitization of the images, which occurred at CUNY in New York. (*Id.* ¶ 2). Again according to the FBI 302s contained in the discovery materials, the Government has not produced any evidence confirming Cassava's chain of custody of the images, its process for preparing them for submission to the NIH, or whether they were altered in any way before submission.

Third, because it lacks the required digital chain of custody and any witness with personal knowledge, the Government attempts but fails to fill the evidentiary gap through expert comparison of visual similarities. Rule 901(b)(3) requires a comparison to a specimen whose authenticity has already been independently established, and no such specimen here exists.

Likewise, Rule 901(b)(4) relies on distinctive characteristics—such as metadata or hash values—that do not exist. Visual similarities like blotches or smudges cannot substitute for the required foundation. Without these foundational markers, the Government's comparisons amount to speculation, not authentication.

Fourth, Rule 901(b)(9), which addresses authentication of evidence generated or stored in a process or system, likewise cannot save the Government. Even if its forensic examiner testifies that certain images were pulled from Dr. Wang's devices, that proves nothing about whether those specific images were ever transmitted to Cassava, whether they were the actual files submitted to NIH, or whether they were altered at any point in between.

Nevertheless, the Government intends to represent to the jury that it has identified the "source images" for the corresponding NIH applications and publication images. It further claims that, within each set of images, one represents an "original" and another a supposedly manipulated version of that original that predates transmission to Cassava. In doing so, the Government is attempting to identify what it contends are the original files underlying the NIH submissions. Yet it has offered no competent evidence to establish that connection, and without such proof, its characterization of these images cannot satisfy Rule 901's authentication requirement. Unless and until the Government can demonstrate outside of the jury's presence that these images are the authentic source images for the NIH applications, the Government should be precluded from identifying or referring to them as any kind of source image.

ARGUMENT

The Government Cannot Authenticate Images as Source Images Under FRE 901

The images the Government claims to be source images cannot withstand the threshold requirement of authentication as source images under FRE 901. Under normal circumstances, a

proponent of an image is attempting to demonstrate under FRE 901 that a source image is a final image. Put simply, that image A = image B. Here, the Government is trying to show that the final image is an altered version of the source image. That is, A + alteration = B. The Government's whole point is, A ≠ B. But before the Government can compare A and B, it must show the necessary predicate that A = A. Without such a threshold showing that A is the source image of B, the Government's argument that A ≠ B is wholly irrelevant and highly prejudicial to Dr. Wang.

None of the methods described in FRE 901(b), whether used individually or together, provide the necessary foundation to establish authenticity of the Government's proffered images as "source images." The Government cannot rely on witness testimony, expert comparison, the presence of commonalities in the images themselves, or the testimony of the forensic examiner that extracted the images. This fundamental failure to establish authenticity leaves the Government's case fatally flawed, and unless and until the Government can demonstrate otherwise, any reference to the images as source images must be excluded.

FRE 901(a) states that "in general, to satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is." *United States v. Vidacak*, 553 F.3d 344, 349 (4th Cir. 2009) (quoting Fed. R. Evid. 901(a)). While the factual determination of whether evidence is that which the proponent claims is reserved for the jury, *United States v. Branch*, 970 F.2d 1368, 1370 (4th Cir. 1992), the district court acts "as gatekeeper in assessing whether the proponent has offered a satisfactory foundation from which the jury could reasonably find that the evidence is authentic." *Vidacak*, 553 F.3d at 349 (citing *United States v. Branch*, 970 F.2d 1368, 1371 (4th Cir. 1992); *United States v. Safavian*, 435 F. Supp. 2d 36, 38 (D.D.C. 2006)). Although the burden to authenticate under FRE 901 requires only a prima facie showing, consistent with the

court's "gatekeeping" function, the proponent must still present some reliable evidence supporting authenticity. *Id*; *United States v. Banks*, 29 F.4th 168, 181 (4th Cir. 2022) (quoting *United States v. Recio*, 884 F.3d 230, 236 (4th Cir. 2018); *United States v. Hassan*, 742 F.3d 104, 133 (4th Cir. 2014)).

This framework applies with equal force to electronically stored information ("ESI"). While FRE 901 does not impose heightened standards for ESI, the nature of digital data often necessitates greater scrutiny than that required for the authentication of, for example, a "hard copy" document, including particularized attention to metadata, chain of custody, and source reliability. *See Am. Exp. Travel Related Servs. v. Vinhnee (In re Vinhnee)*, 336 B.R. 437, 444-45 (B.A.P. 9th Cir. 2005) (observing that while "[a]uthenticating a paperless electronic record, in principle, poses the same issue as for a paper record, the only difference being the format in which the record is maintained . . . . "[t]he paperless electronic record involves a difference in the format of the record that presents more complicated variations on the authentication problem than for paper records"); *see also* MANUAL FOR COMPLEX LITIGATION at § 11.447 ("In general, the Federal Rules of Evidence apply to computerized data as they do to other types of evidence. Computerized data, however, raise unique issues concerning accuracy and authenticity. . . . The integrity of data may also be compromised in the course of discovery by improper search and retrieval techniques, data conversion, or mishandling. The proponent of computerized evidence has the burden of laying a proper foundation by establishing its accuracy. The judge should therefore consider the accuracy and reliability of computerized evidence, including any necessary discovery during pretrial proceedings, so that challenges to the evidence are not made for the first time at trial."). Indeed, courts are placing greater demands on proponents of ESI to establish a strong foundational basis for authentication—more stringent than what has traditionally been required for evidence derived

from non-electronic sources. *See United States v. Shah*, 125 F. Supp. 3d 570, 577 (E.D.N.C. 2015) (acknowledging the "special problems of authenticity inherent in electronic communications" and noting that, because of these issues, "courts have demanded a somewhat more stringent showing than would be required for 'ordinary' evidence."); *see, e.g.*, *Hassan*, 742 F.3d at 133-34 (holding no abuse of discretion where trial court required the Government to connect electronic records to defendant's email and IP address); WEINSTEIN at § 900.06[3] (explaining the need for detailed foundational evidence increases when data is processed; highlighting risks including data input errors, software defects, system security, and incomplete chain of custody; emphasizing the necessity of demonstrating the accuracy, reliability, and integrity of computer-based evidence)).

FRE 901(b) offers illustrative examples of acceptable methods of authentication including (1) testimony of a witness with knowledge, (2) nonexpert opinion on handwriting, (3) comparison by the trier or expert witness, (4) distinctive characteristics and the like, (5) voice identification, (6) telephone conversations, (7) public records or reports, (8) ancient documents or data compilation, (9) process or system and (10) provided by statute or rule. Fed. R. Evid. 901(b). The ten methods identified by FRE 901(b) are non-exclusive. Fed. R. Evid. 901(b) advisory committee's note ("The examples are not intended as an exclusive enumeration of allowable methods but are meant to guide and suggest, leaving room for growth and development in this area of the law.").

Although the illustrative methods of authentication set forth in FRE 901(b) "relate for the most part to [physical] documents," the Advisory Committee expressly acknowledged the growing relevance of computer-generated evidence. *See* Fed. R. Evid. 901(b) advisory committee's note (noting how FRE 901(b)(9) was drafted with "recent developments" in computer technology in mind and is intended to address the authentication of computer printouts and data generated by

electronic processes). In practice, courts have applied various methods listed in FRE 901(b) to electronic evidence, specifically 901(b)(1) (witness with personal knowledge), 901(b)(3) (expert testimony), 901(b)(4) (distinctive characteristics), and 901(b)(9) (system or process capable of producing a reliable result). *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 559 (D. Md. 2007) ("The methods of authentication most likely to be appropriate for computerized records are 901(b)(1) . . . 901(b)(3) . . . 901(b)(4) . . . and 901(b)(9)").

1. *The Government Cannot Authenticate the Images as "Source Images" Because There Is No Digital Continuity Under Rule 901.*

To satisfy Rule 901, the proponent of evidence must make a prima facie showing that "the item is what the proponent claims it is." Fed. R. Evid. 901(a); *Vidacak*, 553 F.3d at 349. When the evidence is ESI, courts have recognized that authentication requires particularized attention to metadata, chain of custody, and other forensic markers that can reliably link a file to its claimed origin. *See Lorraine*, 241 F.R.D. at 546–47 (explaining that metadata, hash values, and other electronic identifiers are central to authentication of digital images). Without such continuity, the proponent fails at the threshold stage.

Here, the Government cannot carry the prima facie burden that 901 requires. As Alyssa Lisiewski's expert analysis makes clear, the files did not move seamlessly from a laboratory scanner into an NIH submission. Instead, the Western blot films were first scanned into high-resolution .tiff images, then converted into compressed JPEG files using ImageJ. (Ex. 1 at 3-4). From there, the images were cropped and adjusted (permissibly) in Photoshop and finally merged into labeled figures in PowerPoint slides for email transmission. (*Id.*).

The critical break in continuity occurred at the final stage. Once merged into PowerPoint, the individual images no longer existed as separate entities. (*Id.* at 6-10). Rather, they were flattened into a composite, with no way to extract or assign them hash values individually. (*Id.*).

As Ms. Lisewski's expert report explains, "the merged content within these files could not be hashed at the individual row or 'white box' level, and there was no available method to match the images based on hash value. At the time of Ankura's analysis, [its] digital forensic expert was not aware of any digital forensic process capable of identifying and isolating individual image components by hash value." (*Id.* at 10). In short, there is no forensically sound method available to confirm that the images the Government now points to as "source images" are in fact the same files underlying the NIH submissions.

2. *The Government Cannot Authenticate the Images as Source Images Under FRE 901(b)(1) Because No Witness Has Personal Knowledge.*

FRE 901(b)(1) permits authentication through "[t]estimony that a matter is what it is claimed to be." Fed. R. Evid. 901(b). The advisory committee's note explains that this provision "contemplates a broad spectrum," including "testimony of a witness who was present at the signing of a document." Fed. R. Evid. 901(a) advisory committee's note. A witness may acquire sufficient knowledge by participating in or observing the event reflected by the exhibit. WEINSTEIN at § 901.03[2].

Courts addressing the admissibility of electronic evidence have similarly acknowledged that it may be authenticated by a witness with personal knowledge. *See e.g., Melo v. Zumper, Inc.*, 439 F. Supp. 3d 683, 695 (E.D. Va. 2020) (holding that screenshots included in an affidavit were properly authenticated through testimony of a witness with personal knowledge regarding the appearance, function of the company website, and the operation of the systems through which user information is submitted and stored, including the process of creating new user accounts); *see also United States v. Patterson*, 277 F.3d 709, 713 (4th Cir. 2002) (explaining that photographs are typically authenticated through eyewitness testimony confirming the image accurately depicts the scene or expert testimony establishing that the image was produced by a reliable process).

However, the authenticating witness must provide factual specificity concerning the process by which the electronically stored information was created, acquired, maintained, and preserved without alteration, or the manner in which it was produced by a system or process designed to ensure accuracy. *Lorraine*, 241 F.R.D. at 545-46. Boilerplate, conclusory statements that merely recite the elements of, for example, the business record exception under FRE 803(6) or the public record exception under FRE 803(8) are insufficient. *Id.; see, e.g.*, *Wady v. Provident Life and Accident Ins. Co. of Am.*, 216 F. Supp. 2d 1060 (C.D. Cal. 2002) (sustaining objection to affidavit of plaintiff's witness attempting to authenticate documents taken from the defendant's website because the affiant lacked personal knowledge of who maintained the website or authored the documents); *Patterson*, 277 F.3d at 713 (confirming that because "there was no Government witness who had examined Patterson's fingers and could verify that they were accurately rendered on the Tenprinter image" the photograph could not be authenticated"); *Dillon v. BMO Harris Bank, N.A.*, 173 F. Supp. 3d 258 (M.D.N.C. 2016) (noting that the witness could not competently testify to the contents of an agreement because he did not read it, did not recall seeing an arbitration clause, and remembered only the loan amount); *Webster v. ACB Receivables Mgmt., Inc.*, 15 F. Supp. 3d 619, 634 (D. Md. 2014) (order of Gauvey, Mag. J.) (declining to credit plaintiff's purported admission where plaintiff lacked personal knowledge); *Hagen v. United States*, 485 F. Supp. 2d 622, 626 (D. Md. 2007) (declining to consider testimony about signature cards where witness admitted he had no personal knowledge of whether plaintiff signed the cards); *Vidacak*, 553 F.3d at 350 (holding that foreign records purporting to show defendant's Israeli criminal history were not properly authenticated where the U.S. immigration officer who testified had requested, but was not personally familiar with, the documents); *see generally* Fed. R. Evid. 602 (requiring personal knowledge as a condition of testimony).

The Government cannot satisfy its authentication burden under Federal Rule of Evidence 901(b)(1) to show that the images it points to are the source images for what Cassava ultimately submitted to the NIH. In this case, the Government does not appear to have located a single percipient witness who was involved in the digitization or formatting of the images. Similarly, while Cassava ultimately received image files prior to submission to the NIH, the Government has identified no witness from Cassava who is willing to testify to the authenticity of those images, affirming that the images were unaltered after receipt, or explaining how they were handled, stored, or formatted prior to submission to NIH. In the absence of such testimony from anyone at Cassava, the Government cannot fill the evidentiary gap that exists between the images allegedly received by Cassava and the versions submitted in the NIH application.

This lack of testimony leaves a critical break in the chain of knowledge required under Rule 901(b)(1). Without a witness who can affirmatively testify that the images at issue are what the Government claims they are—images created by Dr. Wang and transmitted without alteration to Cassava and then without alteration to the NIH—the Government cannot meet its burden. Rule 901(b)(1) requires more than speculation or inference; it requires direct testimony by someone with personal knowledge. In the absence of such testimony, the images remain unauthenticated as source images to the NIH applications and testimony, evidence, or reference to them as source images must be excluded.

3. *The Government Cannot Authenticate Images as Source Images Under Rule 901(b)(3) or 901(b)(4) because the NIH-submitted images are insufficient baseline comparison images*

FRE 901(b)(3) and 901(b)(4) both permit authentication of evidence by comparison, but through distinct pathways. Rule 901(b)(3) allows authentication via comparison by an expert or the trier of fact with a "specimen which has been authenticated." Fed. R. Evid. 901(b)(3); *see*

Lorraine, 241 F.R.D. at 546 (explaining that, for this method to apply, there must first be a comparison specimen whose authenticity has been independently established through reliable means such as metadata, chain of custody, or forensic validation). Rule 901(b)(4) permits authentication based on the item's "appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances." Fed. R. Evid. 901(b)(4).

Both rules presuppose the presence of identifiable and reliable circumstantial features—such as hash values or an independently established source image—that can independently corroborate an image's origin and integrity. But here, there are no comparable hash values. (Ex. 1 at 10). And there are no independently established source images. As a result, the Government's expert, Dr. Paul Brookes, attempts to authenticate "source images" by pointing to supposed visual similarities to the NIH-submitted versions—such as shared blotches or smudges typically visible only after extreme adjustment or enlargement. But Dr. Brookes' analysis based on the image's visual resemblance to the NIH image is insufficient because the very question at issue is whether the "source image" is what the Government claims it to be—the proper source for comparison with the NIH image. If it is not, then shared blotches or smudges prove nothing. As the Government's discovery production makes clear, Dr. Wang's laboratory produced thousands if not tens of thousands of Western blot images in the relevant time period, and Dr. Brookes does not appear to claim to have reviewed and eliminated all of those as potential "source images." Nor does Dr. Brookes claim to have reviewed the physical Western blot films from which the scanned images were created, a forensic copy of the scanner memory used to convert those films to digital, or any forensic remnants of those images' analysis in Image J or Photoshop. Dr. Brookes simply cannot eliminate the possibility that his analysis is not using the correct "source images."

Dr. Brookes repeatedly concedes as much—that he is not, and cannot be, certain he has ever analyzed the actual original image for any Western blot at issue. In each report describing the "three-stage pipeline" methodology he devised for this case, Dr. Brookes expressly qualifies his conclusions with the caveat that they are made only "in the absence of original blot images showing the bands of interest as they appear in the final figure." (See, e.g., Exhibit 2 at 5).

Moreover, when Special Agent Weeks interviewed Dr. Brookes after Dr. Wang filed his initial motion in limine challenging Dr. Brookes' testimony, Dr. Brookes again acknowledged the limits of his review. In response to Dr. Wang's position that certain relevant images might be missing, Dr. Brookes stated only that he analyzed the images provided to him by Special Agent Weeks and "also reviewed a large database of images associated with Dr. Wang for relevant or related images." (Exhibit 3 at 2). He stopped well short of affirming that the materials he reviewed necessarily included the true originals or a complete set of the relevant Western blot images. His own admissions confirm that his opinions rest on an incomplete and uncertain record, not on analysis of authenticated originals.

4. The Government Cannot Authenticate Images as Source Images Under Rule 901(b)(9) because Location on a Device Does Not Establish Authenticity.

Rule 901(b)(9) permits authentication of evidence through proof "that a process or system produces an accurate result." Fed. R. Evid. 901(b)(9). But even if the Government were to call a forensic examiner to testify that certain images were recovered from Dr. Wang's devices, that testimony along would not establish that those images are the same "source images" later used in NIH submissions. The presence of a file on a device says nothing about whether it was the file transmitted to Cassava, whether Cassava altered or reformatted the image before submission, or whether the NIH figures were created for a different version all together. Without evidence bridging these critical gaps, Rule 901(b)(9) cannot supply the foundation the Government lacks.

CONCLUSION

The Government must establish that images obtained from Dr. Wang are the "source images" for those submitted to the NIH. Dr. Wang respectfully requests that this Court preclude the Government from eliciting testimony, admitting exhibits, referring to in opening statements or closing arguments, or alluding to in any other way that images from Dr. Wang are "source images" for NIH images unless and until the Government sufficiently meets its burden under Rule 901(b) outside the jury's presence.

Dated: September 24, 2025

Respectfully submitted,

/s/ Joanne Zimolzak

Jennifer L. Beidel (*Pro Hac Vice*)
Mark Chutkow (*Pro Hac Vice*)
Timothy Caprez (*Pro Hac Vice)*
Emma Blackwood (*Pro Hac Vice*)
DYKEMA GOSSETT PLLC
39577 Woodward Avenue Suite 300
Bloomfield Hills, MI 48304
(248) 203-0700
jbeidel@dykema.com
mchutkow@dykema.com
tcaprez@dykema.com
eblackwood@dykema.com

Joanne Zimolzak (19342)
DYKEMA GOSSETT PLLC
1301 K Street NW
Suite 1100 West
Washington, D.C. 20005
(202) 906-8600
jzimolzak@dykema.com

Counsel for Dr. Hoau-Yan Wang